Risiko der Verarbeitung und Datenschutzverletzungen WS 18/19

Susan Gonscherowski

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Gliederung

- Risiko im Datenschutz
  - Begriff, Dimensionen, Beurteilung
  - Typische Datenschutzrisiken
- Datenschutzverletzung
  - Begriff
  - Formale und inhaltliche Anforderungen an Meldung und Benachrichtigung
- Fragen

Der Begriff „Risiko" im Datenschutz

Ein Grundrechts-Eingriff liegt schon bei Durchführung eines personenbezogenen Verfahrens vor!

- Das gilt auch dann, wenn dieses
  - durch eine Rechtsgrundlage gerechtfertigt ist und
  - nachgewiesen sichere IT eingesetzt wird.
- Insofern liegt schon ein „**eingetretenes Risiko**" vor.

➢ Der Eingriff muss dann durch technische und organisatorische Schutzmaßnahmen auf das unbedingt erforderliche Maß verringert werden.

- Eingriff erzeugt Risiken und unmittelbare (physische, materielle, immaterielle) Folgen für die einzelnen Betroffenen
- Mittelbare Folgen für alle Personen aufgrund gesellschaftlicher Strukturschädigungen

Der Begriff „Eingriff"

- Jedes **staatliche Handeln**, das zu einer Beeinträchtigung des durch ein Grundrecht geschützten Lebensbereichs (Schutzbereich) führt

oder

- Das kausal und zurechenbar dem Grundrechtsträger ein Verhalten erschwert, das vom Schutzbereich eines Grundrechts erfasst wird.

- Mittelbare Drittwirkung stellt Grundrechtswirkung zwischen Privaten sicher

Risiko in der DSGVO

- Risiko im Sinne der DSGVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann.
- Es hat zwei Dimensionen:
  1. die Schwere des Schadens und
  2. die Wahrscheinlichkeit,

  dass das Ereignis und die Folgeschäden eintreten.

Eintrittswahrscheinlichkeit

- Risiko für Schutz personenbezogener Daten durch jede Form der Datenverarbeitung

! Eintrittswahrscheinlichkeit = 100% !

- Schaden ist, z.B. Kontrollverlust (Verletzung der Vertraulichkeit, Nichtverkettung, Transparenz) Rufschädigung (Verletzung der Integrität), finanzieller Verlust, Verletzung von Berufsgeheimnissen, Beeinträchtigung von Grundrechten wie freie Meinungsäußerung (chilling effect)

Faktoren der Risikobeurteilung

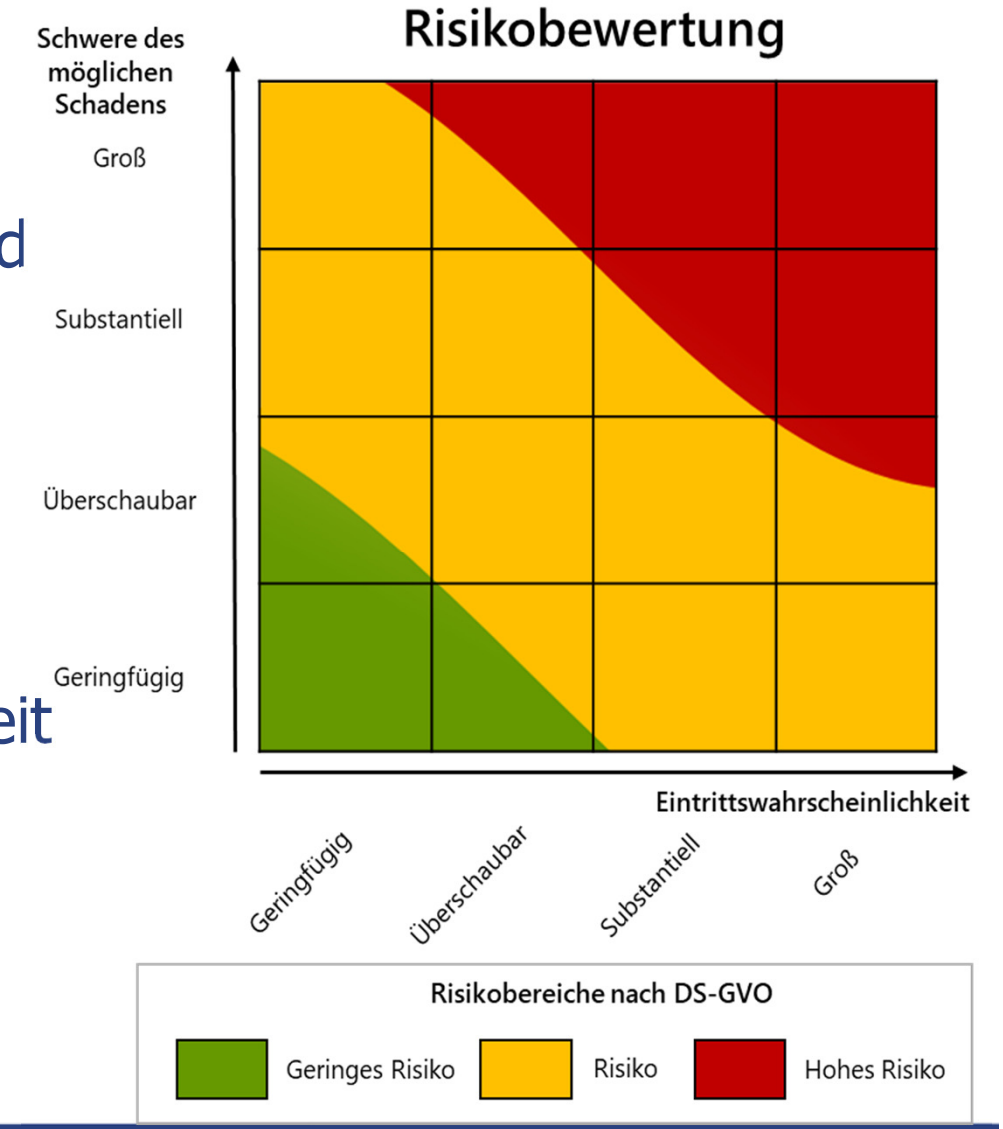
- Schwere möglicher Schäden
  - Wesentliche Faktoren:
    - Schützenswerte Personen/Daten (Kinder, Beschäftigte, Artt. 9, 10)
    - Eindeutig identifizierende Daten, z.B. PKZ
    - Profiling
    - Reversibilität des Schadens
    - Systematische Überwachung
    - Anzahl der Personen, Datensätze, Merkmale in Datensatz oder geographische Abdeckung

Risikobeurteilung

1. Risikoidentifikation
   - Welche Schäden können entstehen?
   - Durch welche Ereignisse können Schäden entstehen?
   - Durch welche Handlungen/Umstände können Ereignisse eintreten?
2. Abschätzung von
   - Eintrittswahrscheinlichkeit
   - Schwere möglicher Schäden
3. Zuordnung zu Risikoabstufungen

Risikobereiche

- Risiko
  - Risiko für die Rechte und Freiheiten des/der **Betroffenen**
  - Faktoren sind Schwere des Schadens (Schadenshöhe) und Eintrittswahrscheinlichkeit



7 typische Risiken im Datenschutz

Risiko 1	Risiko 2	Risiko 3	Risiko 4	Risiko 5	Risiko 6	Risiko 7
Eine Organisation betreibt ein **nicht legitimes personenbe-zogenes Verfahren.**	Die **Schwere des Grundrechtseingriffs** durch ein legitimes pbV wird nicht oder falsch bestimmt, Rechtsgrundlage reicht nicht oder wurde unzureichend geprüft, Die Verantwortungsüber-nahme ist unklar.	Eine Organisation betreibt ein im Grundsatz ordnungsgemäßes pbV, **dehnt oder ändert jedoch den Zweck** (Vorratsdatenspeic herung, Big Data).	Eine Organisation betreibt für ein pbV **keine hinreichend wirksamen Maßnahmen der IT-Sicherheit.**	Eine Organisation betreibt für ein pbV die Maßnahmen der **IT-Sicherheit nicht grundrechts-konform**.	Das **Angreifermodell** bzgl. anderer (befugt) zugreifender Organisationen (z.B. Sicherheitsbehör den) ist **falsch oder unterkomplex** angelegt.	Die pbV von Organisatio nen werden **nicht ausreichend geprüft und beurteilt.**

Risiko 1 : Legitimität eines Verfahrens ist ungeklärt

- Illegitime Verfahren lassen sich **nicht nachträglich** durch Gesetz, Einwilligungen oder durch das Installieren von Schutzmaßnahmen legitimieren/legalisieren!

Verantwortliche, Datenschutzaufsichtsbehörden und Gerichte müssen die Legitimität von Verfahren(stypen) kontrollieren, prüfen und beurteilen.

Art. 35 DSGVO **Datenschutz-Folgenabschätzung** kann Schutz vor nicht-legitimen Verfahren entfalten, weil konsistenter als bislang jedes Verfahren zu prüfen ist.

- Eintrittswahrscheinlichkeit? Hoch

Durch bspw. Facebook, Google / Apple findet Vollüberwachung von Personen statt; inzw. ist eine kulturelle Gewöhnung an eine Vollüberwachung der menschlichen „Laborratten" (Wehler) und „Zombies" (Kutscha) eingetreten, too big to fail.

- Schwere des Risikos? Hoch

Illegitime Verfahren unterlaufen soziale Schutzvorkehrungen moderner Gesellschaften, sie führen zur **De-legitimierung des Rechts und der Institutionen**, Auslieferung von Personen an Privatorganisationen findet statt, staatliche Exekutive bedient sich zudem der Infrastrukturen und Datenbestände der Kommunikations-unternehmen zur Vollüberwachung der Bürger.

Risiko 2 : Falsche Bestimmung Schwere des Grundrechtseingriffs

Falsche Bestimmung der Schwere eines Grundrechteeingriffs führt zu einer falschen Bestimmung der Wirksamkeit von zu treffenden Schutzmaßnahmen, die die Eingriffsintensität auf das geringstmögliche Maß mildern könnten.

- Empfehlenswert: **Typisierung der Grundrechtseingriffe, um die Schwere einzuordnen** (z.B. „leicht, mittel, schwer"). Bislang jedoch keine Praxis in der Datenschutzaufsicht.

Nicht Sensitivität personenbezogener Daten, sondern Eingriffsintensität ist maßgeblich.

Es bedarf eines umfassenden spezifischen Angreifermodells des Datenschutzes in Abgrenzung zum Angreifermodell der IT-Sicherheit.

- Eintrittswahrscheinlichkeit? Hoch

Weil keine Übung in der juristischen Entscheidungsfindung, und wenn ausnahmsweise doch genutzt dann ist es folgenlos für Bestimmung der Maßnahmen.

- Schwere des Risikos? Hoch

Beeinträchtigt Personen unmittelbar. Eine unangemessen leichte beliebige Verkettbarkeit von Daten unterläuft strukturelle Schutzvorkehrungen moderner Gesellschaften mit der Folge der Zerstörung von Strukturen und Auslieferung von Personen an rechtlich nicht eingefangene Organisationen.

Risiko 3: Zwecküberdehnung bei der Anwendung eines Verfahrens

- Die **Zwecksetzung** muss legitim sein, die **Zweckbestimmung** muss hinreichend eng und prüfbar erfolgen, die **Zwecktrennung** und die **Zweckbindung** erleichtern die operative Umsetzung und die Prüfbarkeit eines Verfahrens.

Die Zweckbestimmung bildet den **definitorischen Kern eines pb Verfahrens**, aus dem heraus die erforderlichen Daten, IT-Systeme und Prozesse sowie die Schutzmaßnahmen zu bestimmen sind.

Zweckdehnung findet durch **häufig übermäßige Ausnutzung der Einwilligung** statt, die als vermeintlich souveräner Akt gesehen wird.

Zweckdehnung/-entfremdung sind in der Praxis von Big Data zum Alltag geworden.

Abhilfe z. B. durch breite Nutzung von anyonymen Transaktions-Credentials in Kommunikations-beziehungen möglich.

- Eintrittswahrscheinlichkeit? Hoch

Eine Organisation, die nicht den maximal möglichen Informationsschatz hebt, gerät im Benchmark mit anderen Organisationen ins Hintertreffen, zumal keine gleichmäßig gestreuten, sondern nur „ungerecht punktuelle" Datenschutzprüfungen erfolgen (dadurch „Marktverzerrung").

- Schwere des Risikos? hoch

Beeinträchtigt Personen unmittelbar. Kein fairer Tausch. Eine Ausweitung der Zweckbestimmungen unterläuft ebenfalls strukturelle Schutzvor-kehrungen moderner Gesellschaften mit der Folge der Auslieferung von Personen an Organisationen.

Risiko 4
Mangelhafte IT-Sicherheitsmaßnahmen

- Die IT- bzw. Informationssicherheit bspw. nach **IT-Grundschutz schützt nur die Assets einer Organisation. Die Organisation sieht sich aber oft nicht selbst als Angreiferin!**

Erwägungsgrund 75 DSGVO:

- Diskriminierung,
- Identitätsdiebstahl oder -betrug,
- Finanzieller Verlust,
- Rufschädigung,
- Wirtschaftliche oder gesellschaftliche Nachteile,
- Erschwerung der Rechtsausübung und Verhinderung der Kontrolle durch betroffene Personen.

- Eintrittswahrscheinlichkeit? Hoch

Die Leitungen von Organisationen wissen inzwischen, dass sie ihre IT mit Schutzmaßnahmen ausstatten müssen. These: Gute IT-Sicherheit = guter Datenschutz ist falsch. Und: **Es gibt keine sichere IT.**

- Schwere des Risikos? Hoch

Ein unbefugter Zugriff auf ein Verfahren (auf Daten, IT-Systeme und Prozesse) führt zu einer beliebigen Datenverarbeitung mit teilweise konkreten **materiellen und immateriellen Schäden und unabsehbaren Folgen** für Betroffene und für Gesellschaft (bspw. Wahlbeeinflussung)

Risiko 5: Mangelhafter Datenschutz bei IT-Sicherheitsmaßnahmen

Das **IT-Sicherheitsmanagement ist etabliert** und hat in den letzten 10 Jahren drastisch an Qualität gewonnen.

Methodisch sind IT-SiBe ungleich besser ausgebildet und ausgerüstet als Datenschutzbeauftragte, sie haben in den Organisationen gestalterisch gleich nach dem CIO den Lead.

- Rechtsdogmatisch muss Datenschutz die IT-Sicherheit führen, in der Praxis läuft es genau umgekehrt.

Ganz schlechte Datenschutz-Awareness bei Administratoren bzw. „IT'lern", diese setzen erfahrungsgemäß Maßnahmen der IT-Sicherheit mit denen des operativen Datenschutz gleich, im Konfliktfall zu Lasten der Betroffenen.

- Eintrittswahrscheinlichkeit? Hoch

IT'ler agieren im Auftrag der Organisationsleitung und verstehen den Unterschied zw. IT-Sicherheit für personenbezogene Daten und operativem Datenschutz als Grundrechteschutz meist nicht.

- Schwere des Risikos? Hoch

Schutzmaßnahmen der IT-Sicherheit im Interesse der Organisation dominieren in der Praxis operative Maßnahmen des Datenschutzes.

Risiko 6
Falsches oder schwaches Angreifermodell

➢ Der **Hauptangreifer ist immer die datenverarbeitende Organisation** selbst.

Darüber hinaus gibt es **weitere typische Angreifer-Organisationen** auf Personen:

- Sicherheitsbehörden
- Leistungsverwaltung
- Bereitsteller von IT-(Infrastruktur)Diensten
- Bereitsteller kritischer Infrastrukturen (wie Energieversorger)
- Versicherungen und Banken
- Forschungsinstitute
- Krankenhäuser, Ärzte, Dienstleister
- Untätige Aufsichtsbehörden
- Hacker
- ...

➢ Eintrittswahrscheinlichkeit? Hoch

Es besteht, im Unterschied zur IT-Sicherheit, keine Übung, auch für Datenschutz ein spezifisches Angreifermodell zu formulieren. Ist eine Provokation, „sich selbst" als primäre Konfliktquelle anzusetzen.

➢ Schwere des Risikos? Hoch

Ein befugter Zugriff auf ein Verfahren (auf Daten, IT-Systeme und Prozesse), auf den der Betroffene keinen Einfluss hat, kann zu einer beliebigen Datenverarbeitung mit teilweise konkreten **materiellen und immateriellen Schäden und unabsehbaren Folgen** für Betroffene und für Gesellschaft führen.

Risiko 7: Mangelhafte Datenschutzkontrolle: Institutionenversagen

Verschiedene Fallkonstellationen möglich:

- Personenbezogene Verfahren werden nicht durch unabhängige Datenschutzaufsichtsbehörden geprüft; oder
- pb Verfahren werden zwar geprüft aber die Prüfungen sind unsystematisch oder setzen methodisch falsch an oder sind unvollständig oder nicht intensiv (Prüfintegrität); oder
- Prüfungen werden zwar integer durchgeführt, aber negative Prüfergebnisse seitens der Datenschutzaufsicht bleiben ohne nachhaltige Konsequenzen für den verantwortlichen Datenverarbeiter; oder
- die Datenschutzaufsicht bringt zwar Konflikte vor Gericht, aber das Gericht entscheidet nicht in der Sache; oder
- das Gericht entscheidet zwar in der Sache, aber die gesetzliche Regelung ist unzureichend.

➢ Eintrittswahrscheinlichkeit? Hoch

Die Zahl integrer externer Datenschutzprüfungen, methodisch integrer Prüfungen sowie datenschutz-relevanter Gerichtsentscheidung ist gemessen an der Zahl der Verstöße verschwindend gering.

➢ Schwere des Risikos? Hoch

Willkürlich erfolgende Sanktionen de-legitimieren das Rechts- und Politiksystem und zerstören dadurch wesentliche gesellschaftliche Schutzstrukturen zur Pazifizierung von Organisationen gegenüber Personen.

Wake up Quiz

- Welche zwei Dimensionen bestimmen jedes Risiko?
- Wie wahrscheinlich ist es, dass durch eine Datenverarbeitung ein Risiko entsteht?

Was ist ein Data Breach?

➢ **Verletzung des Schutzes** personenbezogener Daten ausgelöst durch eine Verletzung der Sicherheit

Vorfall führt zu:

- Vernichtung
- Verlust
- Veränderung
- Offenlegung
- Zugang

Verfügbarkeit

Integrität

Vertraulichkeit

➢ Verletzung der 3 klassischen Schutzziele der **IT-Sicherheit** im Zusammenhang mit der Verarbeitung personenbezogener Daten

➢ Ob **beabsichtigt** oder **unbeabsichtigt** spielt keine Rolle.

➢ **Merke**

Jede Verletzung des Schutzes personenbezogener Daten ist auch ein IT-Sicherheitsvorfall, **aber** nicht jeder IT-Sicherheitsvorfall ist auch ein Datenschutzvorfall.

➢ **Auslöser**:

- Missachtung von Vorgaben
- Unfall oder höhere Gewalt
- Vorsatz

➢ **Folgen** eines Data Breach:

- Kontrollverlust über die eigenen Daten
- Einschränkung von Rechten
- Diskriminierung
- Identitätsdiebstahl oder –betrug
- Aufhebung von Pseudonymisierung
- …

Art. 33 DSGVO - Meldung

(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

(2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.

(3) Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4) Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

(5) Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.

Formale Anforderung an eine Meldung

Art. 33 Abs. 1+2 DSGVO:

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet **der Verantwortliche** unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 **zuständigen Aufsichtsbehörde**,

es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich **nicht** zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine **Begründung für die Verzögerung** beizufügen.

Wenn dem **Auftragsverarbeiter** eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese **dem Verantwortlichen** unverzüglich.

- Was?
  - Verletzung des Schutzes personenbezogener Daten
- Wer?
  - der Verantwortliche
  - Der Auftragsverarbeiter dem Verantwortlichen
- Wann?
  - 0 – 72 Stunden nach bekanntwerden
- Warum?
  - Risiko für Rechte und Freiheiten Betroffener
- Wen?
  - Zuständige Aufsichtsbehörde (Art. 55 DSGVO)

Anforderung an Verarbeitungsverfahren

- Das Verarbeitungsverfahren muss **technische** und **organisatorische** Maßnahmen vorsehen um eine Datenschutzverletzung feststellen zu können.

- Intrusion Detection
- Log files, die auch kontrolliert werden
- Versionskontrollen
- Änderungshistorien
- Zugangs- und Zugriffskontrollen
- Vier-Augen-Prinzip
- Dienstvereinbarungen
- …

- Getroffene Maßnahmen müssen jedoch **verhältnismäßig** sein und dürfen die Rechte, z.B. der Mitarbeiter, nicht unzulässig verletzen.

- es müssen **im Vorfeld** Prozesse festgelegt werden, wie zu im Ernstfall zu reagieren ist
  - Wer muss wen informieren (Gibt es eine Rufbereitschaft?)?
    - Mitarbeiter
    - IT-Sicherheitsverantwortliche
    - Datenschutzbeauftragter
    - Führungsebene
    - Betroffene
    - Aufsichtsbehörde(n)
  - Welche Maßnahmen sind zu ergreifen?
    - Shut down und Neustart?
    - Back up einspielen?
  - Wer kann zusätzliche Maßnahmen bestimmen?
  - Was soll wo und wie dokumentiert werden?
    - Ggf. Papier (Kopiervorlage/Notfallordner)
    - Sofort dokumentieren

Inhaltliche Anforderungen an die Meldung

Art. 33 Abs. 3 DSGVO:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der **Kategorien** und der **ungefähren Zahl der betroffenen Personen**, der **betroffenen Kategorien** und der **ungefähren Zahl** der **betroffenen** personenbezogenen **Datensätze**;

b) den Namen und die Kontaktdaten des **Datenschutzbeauftragten** oder einer sonstigen **Anlaufstelle** für weitere Informationen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur **Behebung der Verletzung** des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur **Abmilderung ihrer möglichen nachteiligen Auswirkungen**.

(4) Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese **Informationen** ohne unangemessene weitere Verzögerung **schrittweise** zur Verfügung stellen.

(5) Der Verantwortliche dokumentiert **Verletzungen** des Schutzes personenbezogener Daten **einschließlich aller im Zusammenhang mit der Verletzung** des Schutzes personenbezogener Daten stehenden **Fakten**, von deren **Auswirkungen** und der ergriffenen **Abhilfemaßnahmen**. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.

- **Aufsichtsbehörden** stellen **Meldeformulare** zur Verfügung
- Informationen, die innerhalb der Meldefrist noch nicht bekannt waren, können schrittweise Nachgereicht werden, **aber** ohne unangemessene Verzögerung
- Dokumentation aller meldepflichtigen Informationen muss in jedem Fall erfolgen, **unabhängig** davon ob eine Meldepflicht des Vorfalls besteht

Art. 34 DSGVO - Benachrichtigung

(1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

(2) Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in Artikel 33 Absatz 3 Buchstaben b, c und d genannten Informationen und Maßnahmen.

(3) Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

a) der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;

b) der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht;

c) dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

(4) Wenn der Verantwortliche die betroffene Person nicht bereits über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, kann die Aufsichtsbehörde unter Berücksichtigung der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko führt, von dem Verantwortlichen verlangen, dies nachzuholen, oder sie kann mit einem Beschluss feststellen, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind.

Formale Anforderungen an Benachrichtigung

Art. 34 Abs. 1+2 DSGVO:

(1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes **Risiko** für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der **Verantwortliche** die **betroffene Person** unverzüglich von der Verletzung.

(2) Die in Absatz 1 genannte **Benachrichtigung** der betroffenen Person beschreibt in **klarer und einfacher Sprache** die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in **Artikel 33 Absatz 3 Buchstaben b, c und d** genannten **Informationen** und **Maßnahmen**.

(4) Wenn der Verantwortliche die betroffene Person nicht bereits über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, kann die **Aufsichtsbehörde** unter Berücksichtigung der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko führt, von dem Verantwortlichen verlangen, dies nachzuholen, oder sie kann mit einem Beschluss feststellen, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind.

- Was?
  - Verletzung des Schutzes personenbezogener Daten
  - Name und Kontaktdaten des DSB oder anderer Kontaktstelle
  - Beschreibung der wahrscheinlichen Folgen
  - Maßnahmen zur Behebung oder Abmilderung der Verletzung und der Auswirkungen
- Wer?
  - der Verantwortliche
- Wann?
  - Sofort
  - Nach Aufforderung durch die Behörde
- Warum?
  - Hohes Risiko für Rechte und Freiheiten Betroffener
- Wen?
  - Betroffene

Ausnahmen von der Benachrichtigung

Art. 34 Abs. 3 DSGVO:

(3) Die **Benachrichtigung** der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

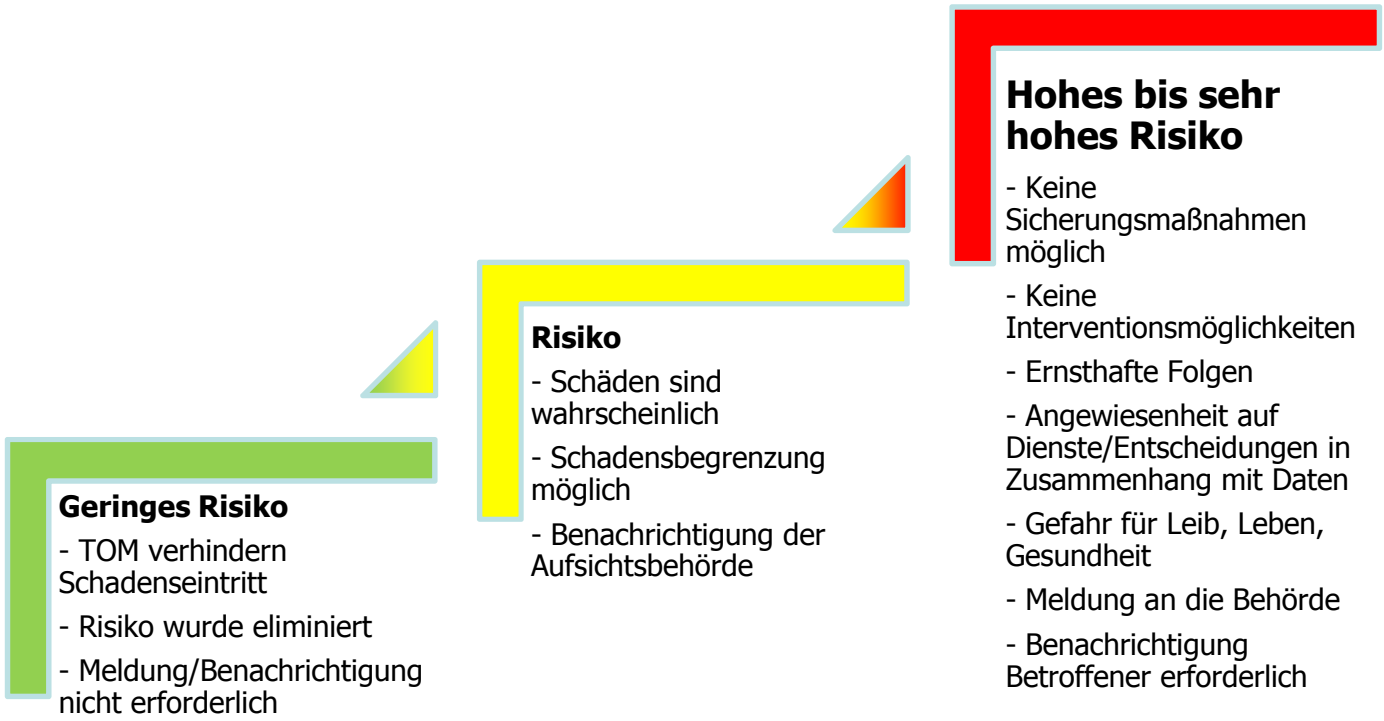
a) der Verantwortliche **geeignete technische und organisatorische Sicherheitsvorkehrungen** getroffen hat und **diese Vorkehrungen** auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;

b) der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass **das hohe Risiko** für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht;

c) dies mit einem **unverhältnismäßigen Aufwand** verbunden wäre. In diesem Fall hat stattdessen eine **öffentliche Bekanntmachung** oder eine **ähnliche Maßnahme** zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

- Präventive Maßnahmen beugen den Folgen vor
  - Bsp.: Verschlüsselung verhindert Kenntnisnahme nach unbefugtem Zugriff
- Ergriffene Maßnahmen heilen die Verletzung
  - Bsp.: Back up stellt von Ransomware verschlüsselte Daten wieder her
- Benachrichtigung der einzelnen Betroffenen ist nicht möglich
  - Bsp.: Wegen eines zerstörten Mailservers stehen keine E-Mail-Adressen mehr zur Verfügung. Es erfolgt eine Meldung auf der Webseite und eine Pressemitteilung an Nachrichtenagenturen

Risiko eines Datenschutzvorfalls



Lücken der Meldung

- DSGVO reguliert Organisationen
- ➢ Datenschutzvorfälle bei Einzelnen (Phishing) sind nicht erfasst

- Art. 33 und 34 DSGVO regeln „akute" Datenschutzvorfälle
- ➢ Risikoänderungen im Lauf der Zeit werden nicht einbezogen
  (Eintrittswahrscheinlichkeit erhöht sich, (Folge-) Schäden werden größer)

- Keine Regelung für Nachfolge von Verantwortlichen
- ➢ Vorfälle werden z.T. gar nicht vom Verantwortlichen erkannt bzw. erst wenn der Verantwortliche nicht mehr existiert

Beispiele

- Equifax: Sozialversicherungsnummern von 145 Mio US-Bürgern öffentlich verfügbar
  (https://www.heise.de/security/meldung/Equifax-Hack-betrifft-noch-mehr-Daten-als-bisher-bekannt-3965066.html)
- Steuern59.ch-App speicherte Angaben und abfotografierte Dokumente öffentlich einsehbar in einer Cloud
  (https://www.heise.de/newsticker/meldung/Schweizer-Steuer-App-speicherte-alle-Daten-oeffentlich-in-der-Cloud-4167240.html)
- MyHeritage: E-Mail-Adressen und Passwörter von 92 Mio Nutzern entwendet
  (https://www.heise.de/security/meldung/DNA-Webseite-MyHeritage-Hacker-kopiert-Daten-von-92-Millionen-Nutzern-4069752.html)
- Sammlung mit 773 Mio Onlinekonten aufgetaucht
  (https://www.heise.de/security/meldung/Passwort-Sammlung-mit-773-Millionen-Online-Konten-im-Netz-aufgetaucht-4279375.html)

Quiz

- Wie lange hat der Verantwortliche Zeit einen Datenschutzvorfall an die Aufsichtsbehörde zu melden?

- Ist ein IT-Sicherheitsvorfall immer ein Data Breach?

Fragen?

Danke für Ihre Aufmerksamkeit

Förderhinweis

Die in diesem Vortrag vorgestellten Erkenntnisse basieren auf Arbeit der folgenden Forschungsprojekte:

www.forum-privatheit.de/

specialprivacy.eu

www.privacyus.eu

https://canvas-project.eu

https://itsec.cs.uni-bonn.de/eidi

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Horizon 2020
European Union funding
for Research & Innovation

Für das Projekt **SPECIAL** (Scalable Policy-awarE linked data arChitecture for prIvacy, trAnsparency and compliance) wurden im Rahmen der Finanzhilfevereinbarung Nr. 731601 Fördermittel aus dem Programm der Europäischen Union für Forschung und Innovation "Horizon 2020" bereit gestellt.

Für das Projekt **Privacy&Us** wurden Fördermittel aus dem Programm der Europäischen Union für Forschung und Innovation "Horizon 2020" unter dem Marie Skłodowska-Curie grant agreement Nr. 675730 im Rahmenprogramm des Marie Skłodowska-Curie Innovative Training Networks (ITN-ETN) bereit gestellt.

Für das Projekt **CANVAS** (Constructing an Alliance for Value-driven Cybersecurity) wurden im Rahmen der Finanzhilfevereinbarung Nr. 700540 Fördermittel aus dem Programm der Europäischen Union für Forschung und Innovation "Horizon 2020" bereit gestellt.